Advancing global critical communications for a safer, more connected world

Follow us on tcca-critical-communications

April 2026

Cybersecurity in Critical Communications

An initial overview

Important Note

The opinions and information given by TCCA in this paper are provided in good faith. Whilst we make every attempt to ensure that the information contained in such documents is correct, TCCA is unable to guarantee the accuracy or completeness of any information contained herein. TCCA, its employees and agents will not be responsible for any loss, however arising, from the use of, or reliance on this information.

Published by TCCA's Cybersecurity Task Force, April 2026

TCCA, Unit 14, Baker's Yard, Christon Road
Gosforth, Newcastle Upon Tyne NE3 1XD, UK
T +44 (0) 191 231 4328 E admin@tcca.info

TCCA Limited is a company incorporated under the Companies Act in England and Wales, company number 04155039.
Registered office: TCCA, Unit 14, Baker's Yard, Christon Road
Gosforth, Newcastle Upon Tyne NE3 1XD, UK

Contents

Section 1 – Introduction 4
1.1 Cyber threat scenario evolution 4

Section 2 – International Organisations driving cybersecurity requirements 5
2.1 Cybersecurity International organisations 5
2.2 Standardisation Organisations 5
2.2.1 International Organisation for Standardisation (ISO) – International Electromechanical Commission (IEC) 5
2.2.2 The 3rd Generation Partnership Project (3GPP) and ETSI 5
2.3 National Standardisation Organisations 6
2.3.1 National Institute of Standards and Technology (NIST) 6
2.4 International Authorities with competence in cyber security 6
2.4.1 European Network and Information Security Agency (ENISA) 6
2.4.2 E-ISAC and EE-ISAC 7
2.5 National Authorities with competence in cyber security 7
2.5.1 USA: Cybersecurity and Infrastructure Security Agency (CISA) 7
2.6 European country specific Cyber Agencies 7

Section 3 – Cybersecurity Frameworks and Methodologies (IT/OT) 8
3.1 Overview of a Cybersecurity Framework (IT and OT) and Methodology 8
3.2 An example of Cybersecurity Framework - NIST CSF 8

Section 4 – Critical Communication Network Deployment models and associated technologies with an initial set of examples of security recommendations 11
4.1 Critical Broadband Networks deployment models and associated technologies 11
4.1.1 Dedicated Mission Critical Network 11
4.1.2 Dedicated Mission Critical Network + shared Mobile Network Operator (MNO) Radio Access Network (RAN) 11
4.1.3 Shared Mission Critical and MNO RAN 11
4.1.4 Dedicated Core shared MNO RAN 12
4.1.5 RAN and part of Core from MNO 12
4.2 Overview of RAN and Core security considerations 12
4.3 Cloud Security 13
4.4 Device 15
4.4.1 Device security 15
4.4.2 Handling of the classified data 15
4.5 Device Management 15
4.5.1 Mobile device management 15
4.5.2 Mobile application management 16
4.5.3 Applications 16

Section 5 – Critical Communication stakeholders and their scope when it comes to Cybersecurity..... 17
5.1 Critical Network Stakeholders and their stake in Cyber 17
5.2 Technology Vendor 17
5.2.1 Technology Security 17
5.3 Network Operators 17
5.3.1 Network/Service Security 17

Section 6 – Critical Communication Asset Matrix 18
6.1 Critical Communication Asset Matrix 18

Section 7 – Conclusions 20

Section 1 – Introduction

The critical communication industry is undergoing a transformation, moving from narrowband networks and services to broadband networks and services. The adoption of 4G and 5G technology in a variety of architectures is the object of investigation and discussion among industry stakeholders: telco, device and application vendors, operators and agencies.

Such a transformation, together with the always evolving set of cyber actors, brings with it also a new set of technologies, assets and ecosystem partners, necessitating adjustments and enhancements to companies' cybersecurity requirements.

This white paper aims to be the first milestone of a joint journey, among all industry stakeholders, towards secure critical communication broadband networks and associated services. It will provide an overview of:

- Section 2 – International Organisations driving cybersecurity requirements (ENISA, CISA, NIST, ISO, 3GPP, TCCA, more)
- Section 3 – Cybersecurity Frameworks and Methodologies (IT/OT)
- Section 4 – Critical Communication Network Deployment models and associated technologies with an initial set of examples of security recommendations
- Section 5 – Critical Communication stakeholders and their scope when it comes to Cybersecurity
- Section 6 – Critical Communication Asset Matrix

1.1 Cyber threat scenario evolution

If in the past professional networks were self-contained, now the scenario is changing, and this technological evolution is bringing both advantages and threats.

Reliance on internet protocol, integration with broadband, exposure to external public networks and integration with commercial mobile networks are bringing benefits in term of flexibility, cost reduction, situational awareness augmentation and use of information, but at the same time are creating favourable situations for threat actors looking for opportunities in a new sector.

The digital landscape in 2026 is marked by rapid technological advancements and geopolitical uncertainties, as highlighted by the 19th edition of the World Economic Forum (WEF) Global Risk Report. Notably, misinformation and cyberattacks emerge as significant perceived risks, reflecting the intricate interplay between technology and geopolitical tensions, further fuelled by advancements in high-impact technologies such as artificial intelligence.

Below are some reports from independent organisations that highlight the threat evolution scenario.

Many other documents produced by cyber security players are available online.

GSMA - Mobile Telecommunications Security Landscape 2025 (https://www.gsma.com/solutions-and-impact/technologies/security/gsma-mobile-telecommunications-security-landscape-2025/)

The Global Risks Report 2026, 21st Edition - Insight Report (https://www.weforum.org/publications/global-risks-report-2026/)

2025 ENISA Threat Landscape Report (ETL) (https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025)

Section 2 – International Organisations driving cybersecurity requirements

2.1 Cybersecurity International organisations

Internationally, multiple organisations are active in the cybersecurity space at a regional, country and industry segment level (ISO/IEC, 3GPP, ENISA; CISA, NIST and more). In the next sections a brief overview of the various organisations is provided with the aim of collocating them in their area of competence and providing some initial guidance to the reader.

2.2 Standardisation Organisations

2.2.1 International Organisation for Standardisation (ISO) – International Electromechanical Commission (IEC)

ISO is a non-governmental organisation formed by the association of standardisation bodies from currently 165 different countries. ISO was founded in 1947 and has its headquarters in Geneva. Each country is represented by a standardisation body. ISO develops globally valid standards in various areas, which are intended to facilitate the cross-border exchange of products and services in the interests of free world trade and technology transfer. Another objective of the standardisation work is to promote transnational technological and scientific cooperation.

The standards developed by ISO are provided in the form of documents. However, ISO is less active in the electrical, electronics and telecommunications fields than other standards organisations such as the International Electrotechnical Commission (IEC) and the International Telecommunication Union (ITU). ISO, IEC and ITU together form the World Standards Cooperation (WSC). The International Organisation for Standardisation also works with the European Committee for Standardisation (CEN), which is responsible for transferring ISO standards into the European standards system.

ISO and IEC have jointly published security relevant standards such as:

- ISO/IEC 27000 Series for Cybersecurity
- ISO/IEC 31010 for Risk assessment
- IEC 62443 Series for ICS
- IEC 63452 (coming in 2026) for Cybersecurity in Rail
- IEC 62351/61850 for Cybersecurity in Energy

just to provide an initial reference list.

2.2.2 The 3rd Generation Partnership Project (3GPP) and ETSI

The 3rd Generation Partnership Project (3GPP) is a joint project of a group of telecommunications associations with the original aim of developing globally applicable specifications for third generation (3G) mobile communications systems. The project was based on the specifications of the Global System for Mobile Communications (GSM) and the International Telecommunication Union (ITU). The partnership project has since expanded its focus to include the maintenance and development of GSM technical specifications and reports.

3GPP brings together telecommunications standards organisations around the world, such as Japan's Association of Radio Industries and Businesses (ARIB) and Telecommunication Technology Committee (TTC), China Communications Standards Association (CCSA), South Korea's Telecommunications Technology Association (TTA), ETSI and the Alliance for Telecommunications Industry Solutions (ATIS) in the USA.

3GPP was officially established in December 1998 when ETSI joined forces with these standardisation and telecommunications organisations with the aim of developing 3G networks. Since its foundation, 3GPP has developed the 3G, 4G and 5G global standards.

ETSI is the European Telecommunications Standards Institute and was founded in 1988 as a non-profit company.

ETSI has more than 800 member organisations worldwide. ETSI produces standards and specifications and is active in all areas relating to information and communications technology (ICT), such as fixed networks, mobile telephony, radio in general, broadcasting and the internet.

3GPP and ETSI have published multiple security standards related to 3G/4G/5G security, examples being:

- (ETSI)/3GPP TS (1)33 501 (Security architecture and procedures for 5G System)
- (ETSI)/3GPP TS (1)33.210 (IP network Layer security)
- (ETSI)/3GPP TS 1)33.310 (Authentication Framework)
- (ETSI)/3GPP TS (1)33.401 (LTE Security Architecture)

just to provide an initial reference list.

2.3 National Standardisation Organisations

2.3.1 National Institute of Standards and Technology (NIST)

The National Institute of Standards and Technology (NIST) is an agency of the US Department of Commerce promoting best practices, innovation, and industrial competitiveness. NIST recommendations serve as a foundation for how technologies and processes are adopted. NIST recommendations, while not binding in the private sphere, nonetheless indicate the direction the US and global industry are taking in areas including information technology, engineering, research, materials use, and measuring. With respect to technology in the public and private sphere, NIST holds considerable influence.

NIST has published relevant cybersecurity standards and the ones below can be used a s initial reference:

- Cybersecurity Framework 2.0 (CSF 2.0)
- SP 800.30 (Guide for Conducting Risk Assessments)

2.4 International Authorities with competence in cyber security

2.4.1 European Network and Information Security Agency (ENISA)

The European Network and Information Security Agency (ENISA) was founded in 2004. Its task is to strengthen information security in the EU. In its activities, ENISA cooperates with national authorities (e.g. BSI in Germany, ACN in Italy, ANSSI in France and more) and institutes.

The EU Cybersecurity Act, which came into force in 2019, has expanded ENISA's responsibilities and competences. Since then, ENISA has been responsible in particular for Network and Information Security Directive (NIS2 - https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02022L2555-20221227) within the European Union and for developing a network and information security for citizens, consumers, businesses and public sector organisations in the European Union. To this end, ENISA is to provide expert advice and solutions to the public and private sectors in EU countries and institutions, organise pan-European cyber crisis exercises, support the development of national cyber security strategies and promote cooperation between IT emergency response teams.

ENISA has also been tasked with developing certification schemes in the field of information security. These cover ICT systems, services and processes in particular and are intended to establish a unified basis for information security in the EU.

Useful material to be used as a reference is listed below:

- https://www.enisa.europa.eu/topics/cyber-threats/threats-and-trends
- https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures
- https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-ransomware-attacks
- https://www.enisa.europa.eu/publications/5g-cybersecurity-standards
- https://www.enisa.europa.eu/publications/nfv-security-in-5g-challenges-and-best-practices

2.4.2 E-ISAC and EE-ISAC

The E-ISAC Home and its European counterpart EE-ISAC Home - EE-ISAC - European Energy - Information Sharing & Analysis Centre, offer the electric industry sharing of security information on how to mitigate complex, constantly evolving threats to the grid. Through the E and EE-ISAC Portal, users can voluntarily post and exchange information about cyber and physical incidents related to grids with full control of how they share it.

These portals are examples of initiatives aimed at sharing cybersecurity information across energy segment stakeholders and harmonising the sharing mechanism as recommended by regulations in multiple geographies.

2.5 National Authorities with competence in cyber security

2.5.1 USA: Cybersecurity and Infrastructure Security Agency (CISA)

The Cybersecurity & Infrastructure Security Agency is a US federal agency established in 2018 through the enactment of the Cybersecurity and Infrastructure Security Agency Act. It reports to the Department of Homeland Security (DHS). CISA's most important task is to detect and combat cyber-attacks against US facilities and infrastructures. Among other things, CISA is responsible for building stable infrastructures and protecting critical infrastructures. Its work supports both the US government and private companies.

CISA's central mission is to detect cyberattacks on US facilities and infrastructures and to combat them. Critical infrastructures are to be protected and strengthened in their resilience so that they can also withstand future threat scenarios. CISA coordinates activities in this area and shares information with government institutions, with industry and with the private sector. It provides cybersecurity tools and incident response services.

CISA Cybersecurity valuable resources can be referenced here:

- https://www.cisa.gov/resources-tools/all-resources-tools

2.6 European country specific Cyber Agencies

In the last years (specifically since when the EC focused on cyber by issuing the first Network Information Security (NIS) directive in 2019) European countries have increased their focus on Cybersecurity by further empowering existing national agencies (National CyberSecurity Center - NCSC in UK or Bundesamt für Sicherheit in der Informationstechnik - BSI In Germany) or by creating new ones like Agenzia per la Cybersicurezza Nazionale - ACN in Italy.

After NIS and NIS2 (active since January 2025) have been issued, each European country has been called to acknowledge the NIS regulation and promulgate national laws to translate it into national rules.

Critical communication providers (if telco operators and/or critical infrastructure owners such as rail, energy and others) are subject to the NIS2. Special regulations may exist on a country basis for public safety agencies and defence organisations.

Reader can refer to national regulations in European countries for a view on local implementation of NIS2 and associated responsibilities as well as to the NIS2 regulation itself.

- NIS2 Directive

Section 3 – Cybersecurity Frameworks and Methodologies (IT/OT)

3.1 Overview of a Cybersecurity Framework (IT and OT) and Methodology

A Cybersecurity Framework is a useful tool that helps critical infrastructure providers as well as agencies to manage the risk in their organisation. The graphic below shows the process the organisation would follow as well as the main areas to be covered.

We want to protect **assets** constituting the physical (terminals, router, switches, radio, etc) and virtual (Mission Critical Push To x (MC-PTx), Operation Support System (OSS), Business Support System (BSS), more) as well as cloud infrastructure (Core, IMS, Registers) that we are going to deploy to enable secure broadband services.

We want to protect them from **threats** which may compromise the 'CIA' of the information:

- Confidentiality of the information
- Integrity of the information
- Availability of the information

by exploiting **vulnerabilities** in the products or the network architecture or the company processes and policies.

Vulnerabilities expose to **risk** of actual attacks such as:

- Denial of Service
- Brute force attacks
- Exploitation
- Ransomware attacks

and more.



Figure1: Cybersecurity Framework

We can protect against **threats** by deploying **safeguards** (**security controls**) in the shape of security capabilities of deployed products, processes, or additional security platforms.

3.2 An example of Cybersecurity Framework - NIST CSF

A risk-based approach like NIST Cybersecurity Framework (CSF) may offer the right versatility with respect to the management of the cybersecurity risk for the deployment of a critical communication infrastructure, as it was primarily designed for critical infrastructure entities of all sizes, sectors, and maturities.

The current NIST CSF version 2.0 has been updated to also help security leaders in organisations using the CSF as a tool for self-assessing current risks.

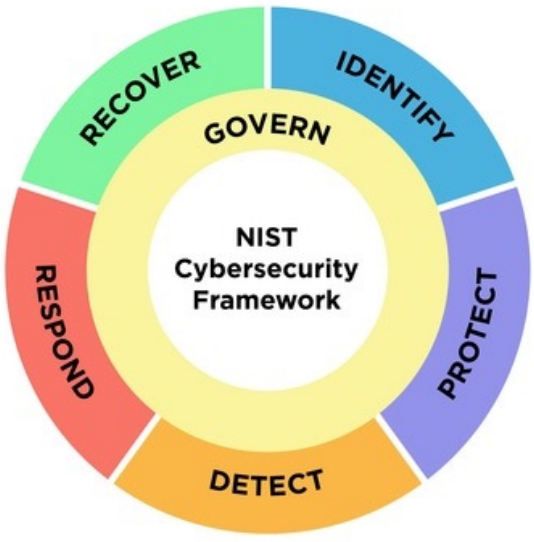


Figure2: NIST CSF

The table below is a valid tool to familiarise with the six functions of NIST Cybersecurity Framework (CSF 2.0 - https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf) and apply it to your own organisation:

- Govern: Develop an organisational cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored.
- Identify: Develop an organisational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.
- Protect: Develop and implement the appropriate safeguards to ensure delivery of services.
- Detect: Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.
- Respond: Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.
- Recover: Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services impaired due to a cybersecurity event.

Function	Category (Category Identifier)	Description
Govern:	Organizational Context (GV.OC):	The circumstances — mission, stakeholder expectations, dependencies, and legal, regulatory, and contractual requirements — surrounding the organization's cybersecurity risk management decisions are understood.
	Risk Management Strategy (GV.RM):	The organization's priorities, constraints, risk tolerance and appetite statements, and assumptions are established, communicated, and used to support operational risk decisions.
	Roles, Responsibilities, and Authorities (GV. RR):	Cybersecurity roles, responsibilities, and authorities to foster accountability, performance assessment, and continuous improvement are established and communicated.
	Policy (GV.PO):	Organizational cybersecurity policy is established, communicated, and enforced.
	Oversight (GV.OV):	Results of organization-wide cybersecurity risk management activities and performance are used to inform, improve, and adjust the risk management strategy.
	Cybersecurity Supply Chain Risk Management (GV.SC):	Cyber supply chain risk management processes are identified, established, managed, monitored, and improved by organizational stakeholders.
Identify	Asset Management (ID.AM):	Assets (e.g., data, hardware, software, systems, facilities, services, people) that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.
	Risk Assessment (ID.RA):	The cybersecurity risk to the organization, assets, and individuals is understood by the organization.
	Improvement (ID.IM):	Improvements to organizational cybersecurity risk management processes, procedures and activities are identified across all CSF Functions.

Function	Category (Category Identifier)	Description
Protect	Identity Management, Authentication, and Access Control (PR.AA):	Access to physical and logical assets is limited to authorized users, services, and hardware and managed commensurate with the assessed risk of unauthorized access.
	Awareness and Training (PR.AT):	The organization's personnel are provided with cybersecurity awareness and training so that they can perform their cybersecurity-related tasks.
	Data Security (PR.DS):	Data are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.
	Platform Security (PR.PS):	The hardware, software (e.g., firmware, operating systems, applications), and services of physical and virtual platforms are managed consistent with the organization's risk strategy to protect their confidentiality, integrity, and availability.
	Technology Infrastructure Resilience (PR.IR):	Security architectures are managed with the organization's risk strategy to protect asset confidentiality, integrity, and availability, and organizational resilience.
Detect	Continuous Monitoring (DE.CM):	Assets are monitored to find anomalies, indicators of compromise, and other potentially adverse events.
	Adverse Event Analysis (DE.AE):	Anomalies, indicators of compromise, and other potentially adverse events are analyzed to characterize the events and detect cybersecurity incidents.
Respond	Incident Management (RS.MA):	Responses to detected cybersecurity incidents are managed.
	Incident Analysis (RS.AN):	Investigations are conducted to ensure effective response and support forensics and recovery activities
	Incident Response Reporting and Communication (RS.CO):	Response activities are coordinated with internal and external stakeholders as required by laws, regulations, or policies
	Incident Mitigation (RS.MI):	Activities are performed to prevent expansion of an event and mitigate its effects.
Recover	Incident Recovery Plan Execution (RC.RP):	Restoration activities are performed to ensure operational availability of systems and services affected by cybersecurity incidents.
	Incident Recovery Communication (RC.CO):	Restoration activities are coordinated with internal and external parties.

Table 1: NIST CSF2.0 functions

Section 4 – Critical Communication Network Deployment models and associated technologies with an initial set of examples of security recommendations

4.1 Critical Broadband Networks deployment models and associated technologies

There are different ways to deploy a mission critical 3GPP standards-based network, depending on whether the mission critical network operator owns all or a share of the required network assets.

In the picture below you can see five different deployment models, and these are briefly described below the picture.

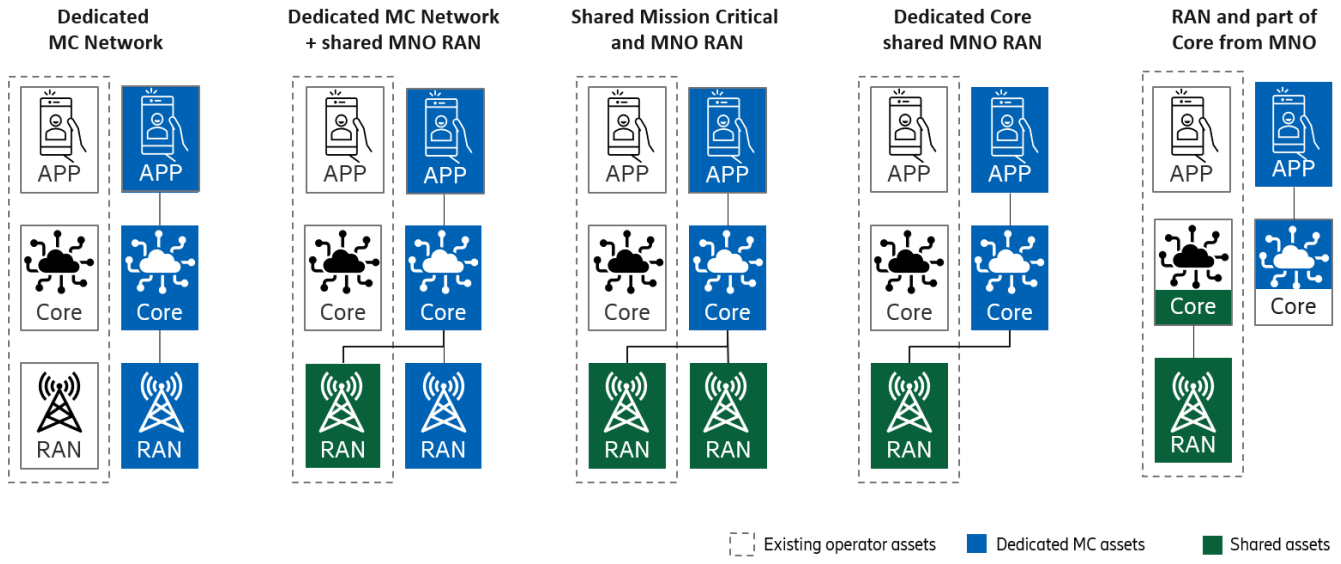


Figure 3: Broadband Critical Networks Deployment models

4.1.1 Dedicated Mission Critical Network

Here a dedicated network is built for a critical communications operator. This can be done together with an existing operator (for example in those countries where the operator owns the frequencies), although the two networks use separate infrastructure, they may share physical sites, transmission and other secure facilities. Alternatively, a dedicated network is built without cooperation with an existing operator with fully dedicated own assets.

Examples of countries adopting this approach are Public Safety and Telefonica in Spain, Publica Safety in UAE and Energy in Saudi Arabia.

4.1.2 Dedicated Mission Critical Network + shared Mobile Network Operator (MNO) Radio Access Network (RAN)

Here a critical communications operator will implement dedicated Core, Application and RAN infrastructure with dedicated spectrum complemented by RAN sharing of a commercial network.

Examples of countries adopting this approach are Public Safety in France, Sweden, Romania and Croatia.

4.1.3 Shared Mission Critical and MNO RAN

In this approach, a RAN network with spectrum owned by the mission critical operator is built. The mission critical operator utilises both its own spectrum and commercial operator spectrum. Further to this the RAN network owned by the mission critical operator can be utilised by the customers of the commercial operator, however critical communication users will have priority access.

Countries adopting this approach are AT&T in the US, serving FirstNet.

4.1.4 Dedicated Core shared MNO RAN

Here the critical communications operator builds dedicated Core and Application infrastructure while an MNO's RAN spectrum and infrastructure is used.

Countries adopting this approach include Erillisverkot in Finland and the ESN in the UK.

4.1.5 RAN and part of Core from MNO

This last model relies on shared use of the commercial network RAN, together with basic core routing capabilities, but complemented with a dedicated core and applications.

4.2 Overview of RAN and Core security considerations

An overview diagram and descriptions for 3GPP and Application Layer Security is shown in the following diagram.

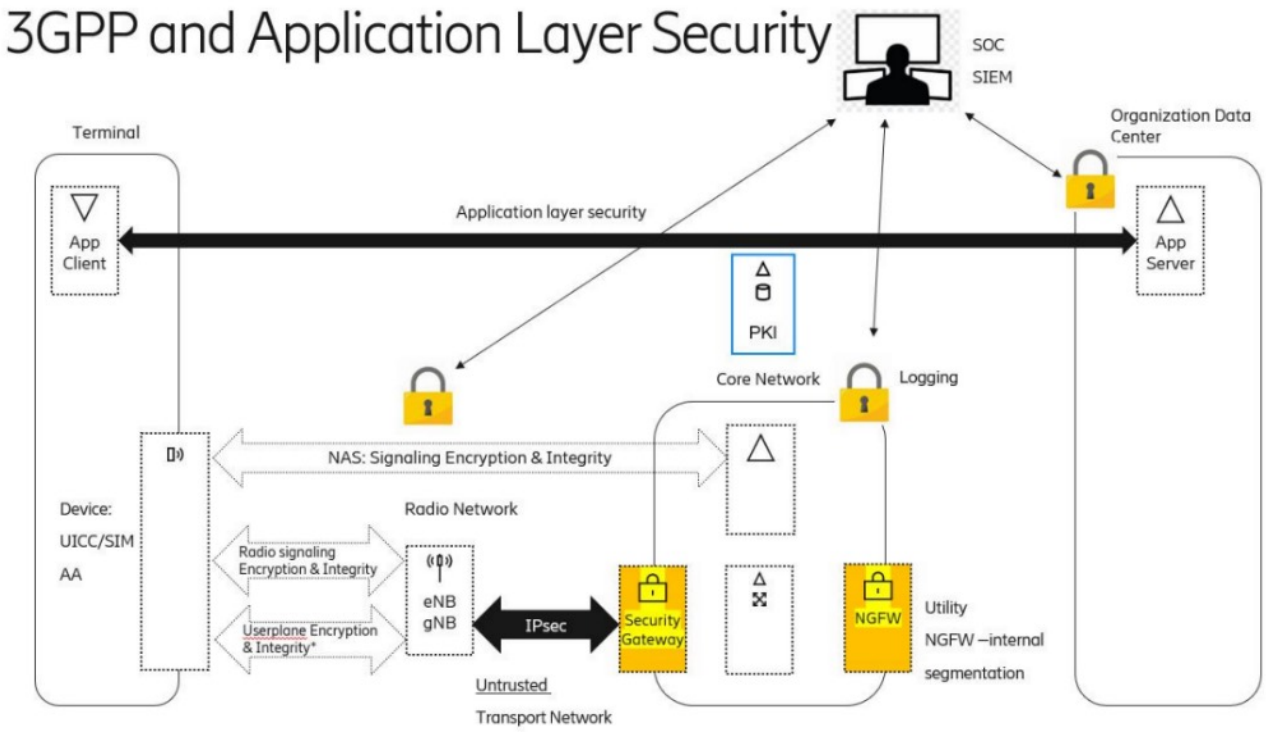


Figure 4:RAN and Core Security

A list of security controls based on 3GPP standards recommendations as well as best practices form well known Cybersecurity frameworks (NIST, IEC62443, more) follows:

- Air interface and Non access Stratum (NAS) encryption according to the Long Term Evolution (LTE) standards using AES-128 encryption and integrity protocols per 3GPP TS 33.401.
- Protected site-to-site communication and transport layer security using IPsec Virtual Private Network (VPN) tunnels for untrusted transport networks.
- Separate security zones for different traffic, e.g., user plane/control plan and Management (O&M) traffic. These are separated using Multi Protocol Label Switching (MPLS) VPN segments and IPSec tunnels per baseband. IPsec is used for untrusted transport terminating on a Security Gateways (SecGW). MPLS VPN is always used in the base design for transport segmentation.
- Core Security implementing mutual Transport Layer Security (mTLS) in 5G core per 3GPP TS 33.501

- Signalling Firewalls (GTP/SS7/Diameter) where applicable as per GSM FS.19/20/21
- Site protection, both physical security and cyber security. Cyber security protection includes using firewalls and intrusion detection systems.
- Telco specific Host based Intrusion Detection Systems (Endpoint Detection and Response/HIDS) as well as Privilege access Management (PAM) are enforced.
- Real-time logging of security and audit events using secure Syslog.
- Authentication, privilege assignment as well logging of all users, both network users and O&M administrators.
- Events are fed to the customer Security Operations Center (SOC) to monitor network security status and act as needed. One will realise that telco specific security events will need to be monitored, and telco specific use cases will be required.

4.3 Cloud Security

Taking into consideration scope of Data Center (DC) solutions, threat identification is an important step to move further. By analysing communication patterns, architecture of defined cloud infrastructure system and gathering possible attack vectors from security expert groups (example OWASP - https://owasp.org/ - or CSA - https://cloudsecurityalliance.org/), there are specific risks emerging from DC inventory elements:

- Defects or vulnerabilities in front-end of DC management applications (Cross Site Scripting (XSS), weak authentication and authorisation)
- Dependency between hosted applications and Virtual Network Functions (VNF) (VNF takeover)
- Escape to host risk in shared / public cloud environments, for those countries who may allow and consider this approach
- Customised Design of compute/control/storage nodes (Software stack vulnerabilities, Configuration weakness due to non-standard practices and operation challenges)
- Usage of 3rd party software e.g. generic containers, libraries (compromising, rogue update)
- Vulnerable control plane – integrity or confidentiality (control to compute communication, storage cluster)
- Software Defined Network (SDN) forwarding/control plane separation e.g. transport security between controller<->switch, profiling of virtual switches
- External Application Programming Interface (API) security – Management And Orchestration (MANO), SDN Designer, Infra web GUI interfaces

As the threats vary based on targets, there are different sources which also enables to assess security risk accurately.

- **External threats** - Attacker can use a vulnerability in the user's Virtual Machine (VM) to take control of it, then move laterally to other VMs in the cloud until the attacker puts their hand on the crown jewels.
- **Threats from a cloud provider** - Attacker can use a cloud misconfiguration for escalation of privileges or information disclosure. For example, an attacker can launch a new VM, and attach a storage volume that was used by a previously running user VM to access sensitive user data.
- **Threats from another tenant** - Attacker can, for example, run an escalation of privileges to escape their VM and take a control over the host and/or other tenants. Attacker can also get access to shared resources, such as storage or network resources.

As a summary of described attack scenarios let's look at the impact in following generalized aspects:

- Integrity, Availability, Confidentiality, Non-Repudiation of telco operator resources (e.g. network, company data)
- Telco Impact (Functionality, Performance etc.) degradation of service offered to customers, outages etc.
- Peered networks – Attack originating from one network where effect is visible elsewhere in the works – (IoT botnets for hire)
- Customer Data – regarding privacy/GDPR rules and using those data for further attacks (Two factor authentication with Banking)

A set of security layers need to be incorporated for securing the system holistically and key security controls relevant to each of the layers of Cloud Infrastructure security can be summarised as described below.

Broadly, such security controls are mapped to five distinct modules of end-to-end security solution approach for cloud infrastructure security.

- Root of trust
  - Integrity protection via attestation
  - Secure boot
  - Vendor certificate
  - Trusted Platform Module (TPM) Hardware (HW) Chip
- Nodes hardening
  - Access Control via Role Based Access Control (RBAC)
  - Intrusion Detection
  - HW resources protection
  - Storage encryption
  - Linux host hardening
- Network security
  - Zoning and segmentation
  - Tenant Separation
  - Traffic filtering
  - Traffic encryption
  - Virtual Firewall (vFW) in perimeter security
- Secure management
  - Certificate Management
  - Malware Protection
  - Identity Management
  - VM image/Software (SW) signing
- Secure orchestration
  - Security Policies automation
  - Cloud remediation
  - Security Monitoring
  - API security

Literature exists on the topic and examples of good practices can be found at the following links:

- Cloud Computing Risk Assessment | ENISA
- https://www.cisa.gov/search?g=telco+cloud+security#gsc.tab=0&gsc.q=telco%20cloud%20security&gsc.page=1:~:text=https%3A//www.cisa.gov/.../security_guidance_for_5g_cloud_infrastructures_p
- https://cloudsecurityalliance.org/blog/2024/10/25/unpacking-the-cloud-security-best-practices-from-cisa-and-the-nsa#

4.4 Device

4.4.1 Device security

Device security has a critical role in ensuring protection of sensitive data. It encompasses the design, implementation, and management of security measures that safeguard the integrity, confidentiality, and availability of the data. Typically, device security consists of multiple layers:

1. Device application security layer is a set of measures and practices implemented to protect mobile applications, end user and sensitive data from various threats and vulnerabilities. Application security aims to prevent unauthorised access, securing communication and safeguarding against malicious activities.
2. Authentication layer includes functionality of applications, user password(s), PIN code(s), two-factor authentication (2FA), Mobile device authenticating service and authentication of connected accessories. Authentication layer is crucial security measure for ensuring that only authorised users can access the device and its functions.
3. Operative System (OS) layer includes application sandboxing and permissions management. Application is granted limited access to system resources, such as files, network connections, and hardware devices. It operates within predefined boundaries and restrictions, enforced by OS. Application has access to limited amount of system calls, APIs or other capabilities. This approach prevents application from performing actions beyond its authorised scope.
4. Data at rest, layer focuses on protecting data stored on the device. It is critical element when preventing unauthorised access in case the device is lost, stolen, or compromised. Data at rest encryption plays a vital role by converting data into an unreadable format that can only be accessed with the appropriate decryption key.
5. Hardware based security, secure booting, secure element, tamper-resistant hardware component providing secure environment for storing sensitive data, like cryptographic keys. Trusted Execution Environment (TEE) is secure area within device that provides a separate execution environment for sensitive operations.
6. Device management (Mobile Device Management (MDM)/Mobile Application Management (MAM)), solutions are commonly used to manage and secure devices. Solution enables enforcing security policies, remotely managing and monitoring devices and perform actions like remote lock, wipe, update firmware over the air and application management.
7. Secure communication including firewall and protocols used (like VPN) to encrypt data transmitted between devices and remote servers.
8. Device provisioning involves the process of setting up and configuring devices within an organisation.
9. Physical Security, measures related to storing facilities of devices and facilities and processes related to device provisioning. Storage and manufacturing facilities are out of scope from this document as well as related processes.
10. Intrusion and malware detection is an activity to detect malicious behaviour of a device, for example caused by governmental actor(s) of a foreign nation trying to intervene with the public safety activities.

4.4.2 Handling of the classified data

When a device is part of the governmental networking, there is sometimes a requirement to handle classified data. In public safety domain this typically means RESTRICTED level of data classification. It should be noted here that any hardware or software handling classified data must be approved via various certification process(es) for handling particular level of classified data. National certifications and accreditations are required for the devices (such as: TCB/FCC in USA, NCSC in UK, BSI in Germany, ANSSI in France...). The communication between two RESTRICTED level devices and/or servers must be properly encrypted when communicating via public networks.

4.5 Device Management

4.5.1 Mobile device management

Mobile device management (MDM) is the process of administering mobile devices: smartphones, sensors, tablets, laptops etc. MDM is deployed into devices by using specific application designed for the purpose. MDM differs

slightly from Enterprise Mobility Management (EMM) and Unified Endpoint Management (UEM): unlike MDM, EMM includes mobile information management. UEM provides device management for endpoints like desktops, printers, IoT devices.

Benefit of mobile device management is improved device security. With MDM, security controls can be implemented and enforced to every single mobile device. Procedures can be established to direct actions in case of suspected security incident. MDM is used to manage trusted applications and devices. Supported MDM solution and devices typically include following functionality:

- Mobile device provisioning – capability to download various configurations to operate the device
- Remote attestation - capability to validate mobile device HW and SW integrity
- Organization application store - organisation controlled private application store, see next chapter.
- Application whitelisting - list of allowed applications for device
- Remote wipe - capability to remotely trigger data wipe in case of severe security incident, for example in the case of stolen or lost device
- Remote lock - capability to lock device user interface in case of security incident
- Retrieve device audit log - systems capability to fetch logs from mobile device to organisations server
- Wireless Local Area Network (WLAN) and Cellular management - admin capability to (dis)allow WLAN connectivity or for example allow only certain type of cellular connections (LTE/5G)

4.5.2 Mobile application management

Mobile application management (MAM) is the process of administering applications of the mobile devices: smartphones, sensors, tablets, laptops etc. MAM is deployed into devices by using specific application and deploying corresponding service: organisation application store to network. MAM is used to manage and distribute trusted applications to devices. Mobile device can support in parallel also application whitelisting or blacklisting, managed by MDM or MAM entity.

4.5.3 Applications

User Equipment (UE) application security is set of measures and practices implemented to protect mobile applications, end user and sensitive data from various threats and vulnerabilities. Application security aims to prevent unauthorised access, securing communication and safeguarding against malware and other malicious activities.

One of the key considerations in application security is ensuring the confidentiality, integrity, and availability of data. It is critical to implement support for encryption techniques to protect data both at rest and in transit. Implementing strong user authentication mechanisms like two-factor authentication will enhance overall security UE and applications.

UE application implementation should be hardened by default. Hardening makes application more difficult to reverse engineer and protects it against tampering. Hardenings can include for example:

- Application integrity checking
- Certificate pinning
- Code hardening
- Data obfuscation
- Emulator detection
- Root and jailbreak detection
- Native code obfuscation

At the very least, software components handling user passwords, PIN codes or two-factor authentication should be hardened.

Section 5 – Critical Communication stakeholders and their scope when it comes to Cybersecurity

5.1 Critical Network Stakeholders and their stake in Cyber

Previous section has set the context to now describe the roles, responsibilities and requirements each stakeholder will have.

5.2 Technology Vendor

5.2.1 Technology Security

There are already many generations of 3GPP Mobile Network technology, 1G –> 5G. Cyber Security is improved in each step of this evolution, and more and more focus is put on Cyber Security as the technology evolves.

The technology vendors role is to develop secure products, based on standards and industry best practices and that are compliant to laws and regulations.

This requires that the vendor has control frameworks that cover the whole product lifecycle from sourcing of components, through development, as well as in deployment and operations in customer networks.

The vendor is also responsible for running a Product Security Incident Response Team (PSIRT) in order to respond to Cyber Security incidents involving the products they provide.

5.3 Network Operators

5.3.1 Network/Service Security

The Mission Critical Network Operator (Operator) needs to assure that their network design is done in a way which is as secure as possible. This includes network segmentation, least privilege access control, perimeter protection to name a few aspects to consider.

The Operator also needs to assure that the network is configured securely, to assure that all the security features of the network is in use.

Once the Network is in operation, the Operator needs to monitor the security configuration to assure a good security posture.

Further to this the network also needs to be monitored to detect potential attacks, this could be done by using tools to monitor logs provided by the network or using security agents in the network.

In addition to the technical capabilities, the Operator also needs to have process which describes who is responsible for what and how a possible security incident is handled within the organisation.

Section 6 – Critical Communication Asset Matrix

6.1 Critical Communication Asset Matrix

A Summary of the list of Critical Networks assets are listed below. Classification of criticality is based on redundancy schemes, impacted users, value of life of the subscriber affected in case of any issue. However, the actual risk level depends on multiple factors that will be assessed by the network operator as well as the service end user once the network is deployed and the service is enabled.

Sub-system	Sensitivity level	Examples of network functions
Core Network Affecting the core network may potentially compromise the confidentiality, availability and integrity of the entire network services. Furthermore, the most sensitive data is transmitted through the core network components.	Critical	Mobility Management Entity (MME), Serving Gateway (S/GW), Packet Network Gateway (P/GW), Access and Mobility Management Function (AMF), Session Management Function (SMF), User Plane Function (UPF) Home Subscriber Server (HSS), Policy Control and Charging Rule Function (PCRF), Unified Data Management (UDM) & Authentication Server Function (AUSF)/ Policy Charging Function (PCF) Diameter Edge Agent (DEA), Security Edge Protection Proxy (SEPP), IP Multimedia Service (IMS), Short Message Service (SMS)
Management and Network orchestration Even though these systems do not carry traffic, they still control important network elements and can therefore be used to conduct malicious acts, such as sabotage and espionage of serious consequences. Moreover, the loss of availability or integrity of these systems and services can significantly disrupt the functioning of mobile networks.	Critical	Radio, Core and Transport OSS Security management systems (Security Information Event Manager (SIEM) or Extended Detection and Response (XDR) for example)
Core Security platforms Since they are controlling the access to the core network elements, once compromised, the malicious attackers may also gain direct access to the core network.	Critical	Endpoint Detection and Response (EDR), Public Key Infrastructure (PKI), Privilege Access Manager (PAM), Authentication Authorization Accounting (AAA), Security Gateway
Radio Access Network A DoS attack could compromise the network only locally.	Moderate/High	Base stations
Transport and transmission They can be physically exposed, vulnerable to wiretapping, though can leverage on geo resilience of routing mechanism and more.	Moderate/High	Local and backbone routers and switches, optical network, fibres
Internetwork exchanges 3GPP foresees protection mechanisms (SEPP for 5G and/or Signalling Firewalls)	Moderate/High	Internetwork exchanges SEPP: Network topology hiding in residing PLMN means enhanced security on the N32 interface.

Sub-system	Sensitivity level	Examples of network functions
Terminals It is critical for the single end user but mitigated by the fact that you may have multiple end users on the same scene. Terminals need to be protected from compromission to safeguard information integrity and confidentiality.	High/Critical	Any device enabling connectivity for the end user
Terminals Device Management	Moderate/High	Mobile Device Management Platform and Terminal Protection Platform
Wearables Not all wearables may be critical like a gas sensor	High/Critical	Camera, smoke sensor, gas sensor, other
Application Servers	Moderate/High	Mission Critical Push to Talk (MCPTT), Video Management Server (VMS), more

Section 7 – Conclusions

The move from narrowband to broadband critical communications comes with great new opportunities but also new risks. The world of critical communications is changing, and the threat landscape is evolving rapidly, maintaining a secure broadband MCX network will bring new challenges that will require cyber security teams to adapt and learn new skills.

Traditional narrowband communications solutions tend to be closed, non-IP-based systems with a more limited attack/threat surface. They tend to be from a single or limited number of vendors possibly benefiting, security wise, from less publicly available or documented source code. It is however evident that the future lies in open standards.

In fact, the new broadband MCX networks are articulated and feature rich entities, multiply interconnected with other systems using open standards that are well understood by threat actors but leverage on the long experience of the 3GPP eco-system that has been securing such networks for decades. The completed broadband communications solution will be from a wider eco-system of vendors than previous narrowband solutions. Take care to validate the security of these vendors and if appropriate consider working with them to improve their security posture to meet your organisational requirements.

To plan for success in transition to broadband critical communications, organisations must make sure they include cyber security at the start of the design and architecture process. Refer to your local national security bodies referred to in this paper for advice, engage with security bodies early and make cyber security front and centre of any vendor's contract. Use a well understood and robust cyber security framework, as discussed above, to guide organisational planning. Organisations should build internal cyber security teams at the start of solution design and before they engage with vendors. Onboard additional cyber security personnel and teams that understand the new threats posed.

A broadband communication solution will include new types of assets that require protecting. Organisations must understand all the assets that will form part of a complete solution, from Radio Access Network (RAN), network core, Mission Critical (MCX) provider, devices, Subscriber Identity Modules (SIM), applications, device management solutions, etc. Make sure that each one is considered in an organisations security planning and that controls are in place around all types of assets. With this number of assets from varied vendors the supply chain is particularly vulnerable to attack. Organisations should include consideration for supply chain attacks in their security posture.

The solution will be complex, organisations will need well practised disaster recovery plans in place. Make sure all vendors have Product Security Incident Response Teams and that the service these teams provide is tested regularly.

As critical broadband communications networks emerge globally, organisations should collaborate to share knowledge and experiences, with a longer-term vision of building international standards to enable an even more robust and secure set of mission critical communications solutions for everyone.